CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

PL-02

Plans de sécurité et de protection de la vie privée des systèmes

Juill. 2026

Votre gouvernement

Québec

PL

Planification de la cybersécurité

Planning

PL-02 — Plans de sécurité et de protection de la vie privée des systèmes (PaFF)

Énoncés :

a. Élaborer des plans de sécurité et de protection de la vie privée pour le système qui :
- **1.** sont conformes à l'architecture d'entreprise de l'organisation
- **2.** définissent explicitement les composants constitutifs du système
- **3.** décrivent le contexte opérationnel du système sur le plan des processus liés à la mission et aux activités
- **4.** identifient les personnes qui assument des responsabilités et des rôles liés au système
- **5.** identifient les types d'informations traitées, stockées et transmises par le système
- **6.** définissent la catégorisation de sécurité du système, y compris la justification à l'appui
- **7.** décrivent les menaces particulières pour le système qui sont préoccupantes pour l'organisation
- **8.** fournissent les résultats de l'évaluation des risques d'atteinte à la vie privée pour les systèmes qui traitent les renseignements personnels
- **9.** décrivent l'environnement opérationnel du système ainsi que les dépendances ou les connexions à d'autres systèmes ou à d'autres composants du système
- **10.** donnent un aperçu des exigences en matière de contrôle de la sécurité et de la protection de la vie privée du système
- **11.** déterminent les bases de référence ou les profils des contrôles pertinents, le cas échéant
- **12.** décrivent les contrôles en place ou prévus pour satisfaire aux exigences de sécurité et de protection de la vie privée, y compris la justification des décisions concernant l'adaptation des contrôles
- **13.** incluent les déterminations des risques découlant des décisions liées à la conception et à l'architecture de sécurité et de protection de la vie privée
- **14.** comprennent des activités liées à la sécurité et à la protection de la vie privée visant le système dont la planification et la coordination doivent être assurées avec [Affectation : personnes ou groupes désignés par l'organisation]
- **15.** sont examinés et approuvés par l'autorité responsable ou une représentante ou un représentant désigné avant leur mise en oeuvre
- **400.** documentent les objectifs organisationnels pour le traitement des renseignements personnels
- **401.** définissent les normes de conservation et d'élimination des documents pour les renseignements personnels stockés dans le système

b. Distribuer des copies des plans et communiquer les changements qui y sont apportés par la suite aux [Affectation : personnel ou rôles définis par l'organisation]
c. Examiner les plans [Affectation : fréquence définie par l'organisation]
d. Mettre à jour les plans pour tenir compte des changements apportés au système et à l'environnement d'exploitation, ou des problèmes soulevés lors de la mise en oeuvre des plans ou des évaluations des contrôles
e. Protéger les plans contre les divulgations ou les modifications non autorisées

Responsable : Aucun

Discussion :

Les plans de sécurité et de protection de la vie privée du système sont adaptés au système et aux composants du système dans la limite d'autorisation définie et contiennent une vue d'ensemble des exigences de sécurité et de protection de la vie privée pour le système et les contrôles sélectionnés pour satisfaire aux exigences. Les plans décrivent l'application prévue de chaque contrôle sélectionné dans le contexte du système avec un niveau suffisant de détail pour mettre en oeuvre correctement le contrôle et en évaluer l'efficacité par la suite. La documentation des contrôles décrit la façon dont les contrôles hybrides et propres au système sont mis en oeuvre, ainsi que les plans et les attentes concernant la fonctionnalité du système. Les plans de sécurité et de protection de la vie privée du système peuvent également être utilisés dans la conception et le développement des systèmes pour appuyer les processus d'ingénierie de la sécurité et de la protection de la vie privée basés sur le cycle de vie. Les plans de sécurité et de protection de la vie privée du système sont des documents évolutifs qui sont mis à jour et adaptés tout au long du cycle de développement du système (par exemple, lors de la détermination des capacités, l'analyse des solutions de rechange, les demandes de propositions et les examens de la conception). La section 2.1 décrit les différents types d'exigences qui touchent les organisations durant le cycle de développement du système et la relation entre les exigences et les contrôles. Les organisations peuvent élaborer un seul plan intégré de sécurité et de protection de la vie privée ou tenir à jour plusieurs plans distincts. Les plans de sécurité et de protection de la vie privée associent les exigences en matière de sécurité et de protection de la vie privée à un ensemble de contrôles et d'améliorations de contrôle. Les plans décrivent également en quoi les contrôles et les améliorations de contrôle satisfont aux exigences en matière de sécurité et de protection de la vie privée, sans pour autant fournir des descriptions détaillées et techniques de la conception ou de la mise en oeuvre de ces contrôles ou de ces améliorations de contrôle. Les plans de sécurité et de protection de la vie privée contiennent suffisamment d'information (y compris des spécifications explicites ou par référence des paramètres d'affectation et de sélection) pour permettre une conception et une mise en oeuvre clairement conformes à ses objectifs et la détermination subséquente des risques qu'ils

représentent, s'ils sont appliqués, pour les activités et les biens de l'organisation, les individus, les autres organisations et le gouvernement. Les plans de sécurité et de protection de la vie privée n'ont pas à être des documents uniques. Ils peuvent être un ensemble de documents, y compris des documents qui existent déjà. Des plans de sécurité et de protection de la vie privée efficaces renvoient largement aux stratégies, aux procédures et à des documents additionnels, comme les spécifications liées à la conception et à la mise en oeuvre, dans lesquels il est possible d'obtenir de plus amples détails. L'utilisation de ces références permet de réduire la documentation associée aux programmes de sécurité et de protection de la vie privée, de même que de conserver l'information relative à la sécurité et à la protection de la vie privée dans d'autres secteurs opérationnels ou de gestion établis, notamment l'architecture d'entreprise, le cycle de développement des systèmes, l'ingénierie des systèmes et l'acquisition. Par exemple, les plans de sécurité n'ont pas à faire mention des plans de secours, des plans d'intervention en cas d'incident ou des processus à suivre advenant une atteinte à la vie privée. Ils peuvent plutôt fournir suffisamment d'information (explicitement et en référence) pour établir quels objectifs ces plans visent à atteindre. Les activités liées à la sécurité et à la protection de la vie privée susceptibles d'exiger de la coordination et de la planification avec d'autres personnes ou groupes au sein de l'organisation comprennent les évaluations, les vérifications, les inspections, la maintenance du matériel et des logiciels, la gestion des acquisitions et des risques liés à la chaîne d'approvisionnement, la gestion des correctifs et la mise à l'essai des plans d'urgence. La planification et la coordination englobent les situations urgentes et celles qui ne le sont pas (c'est-à-dire, planifiées ou non urgentes et non planifiées). Le processus défini par l'organisation pour planifier et coordonner les activités liées à la sécurité et à la protection de la vie privée peut également être inclus dans d'autres documents, le cas échéant.